In the claims: please amend the claims as follows.
This listing of the claims replaces all prior listings.

1. (currently amended) A method for use by a telecommunications terminal ~~(10)~~ in authenticating the telecommunications terminal ~~(10)~~, comprising:

encoding random numbers previously used for authenticating the telecommunications terminal ~~(10)~~, so as to provide a data structure ~~(21)~~ consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

checking the data structure ~~(21)~~ to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure ~~(21)~~ is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

2. (currently amended) A method as in claim 1, wherein in encoding the previously used random numbers, a set of hash functions is used each providing a value in a range equal to the number of components of the data structure ~~(21)~~, and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

3. (previously presented) A method as in claim 1, wherein in encoding the previously used random numbers, the previously used random numbers are used as the pointer values.

4. (currently amended) A method as in claim 1, wherein the data structure ~~(21)~~ is a multi-part data structure ~~(21)~~ with each part having an upper limit on the number of random number values it can indicate as one of the previously used random number values, wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts, and further wherein when an upper limit is reached for the one of the parts, another of the

parts is reset.

5. (currently amended) A computer program product comprising:

a computer readable storage structure embodying computer program code thereon for execution by a computer processor in a terminal ~~(10)~~,

wherein said computer program code includes instructions for performing the method of claim 1.

6. (currently amended) An apparatus for use by a telecommunication terminal ~~(10)~~ in authenticating the telecommunications terminal ~~(10)~~ to an access network, comprising:

means ~~(11 12 14)~~ for encoding random numbers previously used for authenticating the telecommunications terminal ~~(10)~~, so as to provide a data structure ~~(21)~~ consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

means ~~(11 12 14)~~ for checking the data structure ~~(21)~~ to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure ~~(21)~~ is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

7. (currently amended) A system, comprising:

a telecommunication terminal ~~(10)~~, and

a radio access network configured for cellular communication with the telecommunication terminal ~~(10)~~,

wherein the telecommunication terminal ~~(10)~~ includes an apparatus as in claim 6.

8. (currently amended) An apparatus for use by a telecommunication terminal ~~(10)~~ in authenticating the telecommunications terminal ~~(10)~~ to an access network, comprising an authenticator module ~~(14)~~ and one or more Bloom filter modules ~~(11 12)~~, configured to:

encode random numbers previously used for authenticating the telecommunications terminal~~(10)~~, so as to provide a data structure ~~(21)~~ consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

check the data structure ~~(21)~~ to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure ~~(21)~~ is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

9. (currently amended) An apparatus as in claim 8, wherein for encoding the previously used random numbers the authenticator module ~~(14)~~ and one or more Bloom filter modules ~~(11 12)~~ are configured so that a set of hash functions is used each having a range equal to the number of components of the data structure~~(21)~~, and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

10. (previously presented) An apparatus as in claim 8, wherein the previously used random numbers are the pointer values.

11. (currently amended) An apparatus as in claim 8, wherein the data structure ~~(21)~~ is a multi-part data structure ~~(21)~~ with each part having an upper limit on the number of random number values it can indicate as one of the previously used random number values, wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts, and further wherein for encoding the previously used random numbers the authenticator module ~~(14)~~ and one or more Bloom filter modules ~~(11 12)~~ are configured so that when an upper limit is reached for the one of the parts, another of the parts is reset.